

Facial Recognition

Issue: Ongoing media coverage of the RCMP's use of the Clearview AI facial recognition software, in relation to the release of the joint investigation by federal and provincial privacy regulators into Clearview AI.

Proposed Response:

- We are committed to keeping Canadians safe and protecting their privacy rights.
- Strong privacy laws are critical in that effort.
- The RCMP constantly monitors new and evolving technologies in order to keep pace with the evolving methods of criminals, particularly in the area of online child sexual exploitation.
- We are aware of the recently released report of a joint investigation between the Office of the Privacy Commissioner and its provincial counterparts in British Columbia, Alberta and Quebec, which reviewed whether the use of facial recognition technology by Clearview AI complied with Canadian privacy laws.
- The RCMP has been working collaboratively with the Office of the Privacy Commissioner on a separate investigation into the RCMP's use of Clearview AI, which is expected to conclude at a later date.
- The RCMP looks forward to engaging with the Office of the Privacy Commissioner on efforts to develop guidelines on the use of facial recognition technologies by law enforcement.

Facial Recognition

Background

Police in criminal investigations have used traditional facial recognition tools, such as photos of charged persons, for decades. However, technological advances in areas such as biometrics, machine learning and artificial intelligence (AI) have led to the development of more advanced and sophisticated automated facial recognition technology, which can dramatically reduce the amount of time that investigators spend reviewing potential matches.

Automated facial recognition tools are capable of identifying or verifying an individual by comparing and analyzing patterns, shapes and proportions of their facial features and contours. This is a relatively new technology and has been used by some law enforcement agencies.

Clearview AI provides access to a repository of images and any associated metadata that has been collected from publically available websites to facilitate image comparison. Privacy concerns have centered around the legality of law enforcement's use of biometric technologies, including facial recognition, particularly around how the information is collected, used, disclosed, and retained. As a result, on February 21, 2020, the Office of the Privacy Commissioner (OPC), announced an investigation, with its counterparts in Quebec, British Columbia and Alberta, into whether Clearview AI and its use of facial recognition technology complies with Canadian privacy legislation.

On February 27, 2020, the RCMP acknowledged in a public statement that it had recently started to use and explore Clearview AI's facial recognition technology in a limited capacity, in particular by the National Child Exploitation Crime Centre (NCECC). This public statement contradicted a previous media response, which was an error on the part of the RCMP. This error was corrected in the February 27, 2020 statement, wherein the RCMP acknowledged its use of Clearview AI's facial recognition technology.

The RCMP's NCECC has two paid licenses for the Clearview AI application and been using the technology since October 24, 2019. NCECC use has been limited to victim identification for investigations of online child sexual exploitation. To date, this technology has been used in 15 online child sexual exploitation cases, resulting in the successful identification and rescue of two children.

In the February statement, the RCMP also acknowledged that it was aware that some additional units had, on a trial basis, sought to determine whether this technology could enhance criminal investigations. In March, the RCMP issued internal direction that this technology only be used in exigent circumstances for victim identification in child sexual exploitation investigations or in circumstances where threat to life or grievous bodily harm may be imminent. However, since July 2020, the RCMP has stopped the use of this technology, following Clearview AI's withdrawal from the Canadian market.

On February 28, 2020, the OPC announced that it would investigate the RCMP's use of Clearview AI's facial recognition technology. In March 2020, the RCMP was engaged by the Office of the Privacy Commissioner to begin discussions on its use of Clearview AI, and committed to work with the Privacy Commissioner to develop guidelines and policies on the future use of automated facial recognition technologies. While, the OPC was expected to release a report on the findings of the investigation at the end of 2020, this work has not yet concluded and a second report detailing its findings in relation to the RCMPs use of Clearview AI is forthcoming.

On July 8, 2020, a proposed class action was filed with the Federal Court of Canada alleging that Clearview AI collects, copies, stores, discloses and sells facial photos of Canadian residents without their knowledge or consent by using an algorithm to detect the unique face print of an individual. The plaintiff alleges that this is a violation of privacy rights, constitutional rights and their copyright and moral rights as the authors and holders of these rights have not consented to their reproduction and use by Clearview. Furthermore, the plaintiff has alleged that by becoming a customer and client, the RCMP obtained access to and used an illicit database, thus violating the rights of residents and citizens of Canada.

On February 3, 2021, the OPC, with its counterparts in British Columbia, Alberta and Quebec, released the results of their joint investigation into the Clearview AI's use of facial recognition technology. The report concludes that the company violated the federal and provincial privacy laws in Canada in that it collected, used and disclosed Canadian's personal information for inappropriate purposes and collected sensitive biometric information without knowledge or consent.

Contacts:

Prepared by: Kees Bradley, Manager, Cybercrime and Information Sharing Policy, 613-843-5877
Approved by: Stephen White, Deputy Commissioner, Specialized Policing Services, 613-843-4631

Reconnaissance faciale

Sujet : Couverture médiatique sur l'utilisation du logiciel de reconnaissance faciale

Clearview AI par la GRC, à la suite de la publication des résultats d'une enquête menée conjointement par les commissariats à la protection de la vie privée du Canada et de provinces.

Réponse suggérée :

- Nous nous sommes engagés à assurer la sécurité des Canadiens et des Canadiennes et à protéger leur droit à la vie privée.
- À cette fin, il est essentiel de disposer de lois solides en matière de protection de la vie privée.
- Nous sommes au courant que le Commissariat à la protection de la vie privée du Canada et ses homologues de la Colombie-Britannique, de l'Alberta et du Québec ont publié récemment un rapport sur une enquête qu'ils ont menée conjointement afin de déterminer si l'utilisation de la technologie de reconnaissance faciale Clearview AI était conforme aux lois canadiennes en matière de protection de la vie privée.
- La GRC collabore avec le Commissariat à la protection de la vie privée du Canada dans le cadre d'une enquête distincte sur l'utilisation de Clearview AI par la GRC, et cette enquête devrait se conclure à une date ultérieure.
- La GRC est prête à collaborer avec le Commissariat à la protection de la vie privée du Canada à l'élaboration de lignes directrices sur l'utilisation des technologies de reconnaissance faciale par les organismes d'application de la loi.

Reconnaissance faciale

Contexte

Depuis des décennies, la police se sert, dans ses enquêtes criminelles, d'outils traditionnels de reconnaissance faciale comme les photos signalétiques. Or d'importantes avancées technologiques dans des domaines de la biométrie, de l'apprentissage automatique et de l'intelligence artificielle (IA), entre autres, ont mené au développement d'une technologie de reconnaissance faciale automatisée hautement performante et sophistiquée qui permet de réduire considérablement le temps nécessaire à l'examen manuel des correspondances possibles.

Les outils de reconnaissance faciale automatisés permettent d'identifier une personne ou de vérifier l'identité d'une personne en comparant et en analysant les caractéristiques, les formes et les proportions des traits et contours de son visage. Cette technologie, qui est relativement nouvelle, est utilisée par certains organismes d'application de la loi.

Clearview AI fournit un accès à une banque d'images – et des métadonnées connexes – qui proviennent de sites Web accessibles au public afin de faciliter la comparaison d'images. Les principales préoccupations relatives au respect de la vie privée qui ont été exprimées concernent le caractère légal ou non de l'utilisation de technologies biométriques par les forces de l'ordre, y compris la reconnaissance faciale, et plus spécialement la façon dont l'information est recueillie, utilisée, communiquée et conservée. Dans ce contexte, le Commissariat à la protection de la vie privée (CPVP) a, le 21 février 2020, annoncé l'ouverture d'une enquête, à laquelle collaboreront ses homologues du Québec, de l'Alberta et de la Colombie-Britannique, visant à déterminer si Clearview AI et son exploitation de la technologie de reconnaissance faciale est conforme à la législation canadienne en matière de protection de la vie privée.

Le 27 février 2020, dans une déclaration publique, la GRC a reconnu qu'elle avait récemment commencé à explorer et à employer, dans une perspective limitée, la technologie de reconnaissance faciale de Clearview AI, notamment dans les affaires relevant du Centre national contre l'exploitation des enfants (CNEE). Cette déclaration contredisait une réponse faite plus tôt aux médias, réponse qui était une erreur de la part de la GRC. La déclaration faite le 27 février 2020, dans laquelle la GRC reconnaît faire usage de la technologie de reconnaissance faciale de Clearview AI, est venue corriger cette erreur.

Le CNEE de la GRC détient deux licences payantes de l'application Clearview AI, dont elle se sert depuis le 24 octobre 2019. L'utilisation qu'elle en fait se limite à l'identification des victimes dans le cadre d'enquêtes sur l'exploitation sexuelle des enfants en ligne. Jusqu'à présent, cette technologie a été employée dans quinze (15) affaires d'exploitation pédosexuelle en ligne, et elle a permis d'identifier et de secourir deux enfants.

Dans sa déclaration de février, la GRC a également indiqué être courant que certains services tentaient, à titre expérimental, de déterminer si cette technologie pouvait être utile aux enquêtes criminelles. En mars, la GRC a émis une directive interne restreignant l'emploi de cette technologie aux situations d'urgence où il faut impérativement identifier un enfant victime d'exploitation sexuelle ainsi que devant l'imminence d'une menace pour la vie ou d'un risque de blessures graves. Cependant, depuis juillet 2020, la GRC a cessé d'utiliser cette technologie après le retrait de Clearview AI du marché canadien.

Le 28 février 2020, le CPVP a annoncé qu'il enquêterait sur l'usage que la GRC fait de la technologie de reconnaissance faciale de Clearview AI. En mars 2020, la GRC a été approchée par le CPVP pour entamer des discussions à ce sujet et s'est engagée à travailler avec le commissaire à la protection de la vie privée pour élaborer des lignes directrices et des politiques destinées à encadrer l'utilisation, à l'avenir, des technologies de reconnaissance faciale. Le CPVP devait publier un rapport sur les résultats de l'enquête à la fin de 2020, mais ces travaux ne sont pas encore terminés et un deuxième rapport détaillant ses conclusions au sujet de l'utilisation de Clearview AI est attendu.

Le 8 juillet 2020, un projet de recours collectif a été déposé devant la Cour fédérale du Canada, alléguant que Clearview AI recueille, copie, entrepose, communique et vend des photos du visage de résidents canadiens à leur insu et sans leur consentement, en utilisant un algorithme pour détecter l'empreinte faciale d'une personne. La demanderesse allègue qu'il s'agit d'une violation du droit à la vie privée, des droits constitutionnels et des droits moraux et d'auteur puisque les auteurs et les détenteurs de ces droits n'ont pas consenti à la reproduction et à l'utilisation de ces clichés par Clearview. En outre, la demanderesse allègue qu'en devenant client, la GRC a obtenu l'accès à une base de données illicite et l'a utilisée, violant ainsi les droits de résidents et de citoyens du Canada.

Le 3 février 2021, le CPVP et ses homologues de la Colombie-Britannique, de l'Alberta et du Québec ont publié les résultats de leur enquête conjointe sur l'utilisation de la technologie de reconnaissance faciale par Clearview AI. Dans leur rapport, ils concluent que l'entreprise a enfreint les lois provinciales et fédérale sur la protection des renseignements personnels au Canada en recueillant, en utilisant et en communiquant des renseignements personnels de Canadiens à des

fins inacceptables et en recueillant des données biométriques très sensibles à l'insu et sans le
consentement des personnes concernées.

Personnes-ressources :

Préparée par : Kees Bradley, gestionnaire, Cybercriminalité et Politique sur l'échange d'information, 613-843-5877
Approuvée par : Stephen White, sous-commissaire, Services de police spécialisés, 613-843-4631

FACIAL RECOGNITION TECHNOLOGY

- Our government is committed to keeping Canadians safe and protecting their privacy rights
- Strong privacy laws are critical in that effort.
- The Privacy Commissioner is reviewing the use of artificial intelligence technology and we look forward to welcoming and reviewing his report.

If pressed on use of facial recognition

- Continued monitoring of new and evolving technologies will help to keep pace with the methods of criminals, particularly in the area of online child sexual exploitation.
- Guidelines and policies are being developed on the use of biometric technologies by law enforcement.

TECHNOLOGIE DE RECONNAISSANCE FACIALE

- Notre gouvernement est déterminé à assurer la sécurité des Canadiens et à protéger leur droit à la vie privée.
- Pour y arriver, il est essentiel d'adopter des lois rigoureuses en matière de protection des renseignements personnels.
- Le commissaire à la protection de la vie privée examine actuellement le recours à des technologies de l'intelligence artificielle, et nous attendons avec intérêt la publication de son rapport.

Si on insiste sur l'utilisation de la technologie de reconnaissance faciale

- Rester à l'affût des technologies nouvelles et en évolution nous aidera à nous adapter aux méthodes qu'emploient les criminels, en particulier dans le domaine de l'exploitation sexuelle des enfants sur Internet.
- Des lignes directrices et des politiques sont en cours d'élaboration sur l'utilisation des technologies biométriques par les organismes d'application de la loi.

BACKGROUND

- Police in criminal investigations have used traditional facial recognition tools, such as photos of charged persons, for decades. However, technological advances in areas such as biometrics, machine learning and artificial intelligence (AI) have led to the development of more advanced and sophisticated automated facial recognition technology, which can dramatically reduce the amount of time that investigators spend reviewing potential matches.
- Automated facial recognition tools are capable of identifying or verifying an individual by comparing and analyzing patterns, shapes and proportions of their facial features and contours. This is a relatively new technology and has been used by some law enforcement agencies.
- Recently, a number of media outlets have reported on the use of facial recognition software, specifically Clearview AI, by Canadian law enforcement agencies to identify victims of crime or individuals involved in criminal activity.
- Clearview AI provides access to a repository of images and any associated metadata that has been collected from publically available websites to facilitate image comparison. Privacy concerns have centered around the legality of law enforcement's use of biometric technologies, including facial recognition, particularly around how the information is collected, used, disclosed, and retained. As a result, on February 21, 2020, the Office of the Privacy Commissioner (OPC), announced an investigation, with its counterparts in Quebec, British Columbia and Alberta, into whether Clearview AI and its use of facial recognition technology complies with Canadian privacy legislation.
- On February 27, 2020, the RCMP acknowledged in a public statement that it had recently started to use and explore Clearview AI's facial recognition technology in a limited capacity, in particular by the National Child Exploitation Crime Centre (NCECC). This public statement contradicted a previous media response, which was an error on the part of the RCMP. This error was corrected in the February 27, 2020 statement, wherein the RCMP acknowledged its use of Clearview AI's facial recognition technology.
- The RCMP's NCECC has two paid licenses for the Clearview AI application and been using the technology since October 24, 2019. NCECC use has been limited to victim identification for investigations of online child sexual exploitation. To date, this technology has been used in 15 online child sexual exploitation cases, resulting in the successful identification and rescue of two children.
- In the February statement, the RCMP also acknowledged that it was aware that some additional units had, on a trial basis, sought to determine whether this technology could enhance criminal investigations. The RCMP has since issued internal direction that this technology only be used in exigent circumstances for victim identification in child sexual exploitation investigations or in circumstances where threat to life or grievous bodily harm may be imminent.
- On February 28, 2020, the OPC announced that it would investigate the RCMP's use of Clearview AI's facial recognition technology. The RCMP has been engaged by the Office of the Privacy Commissioner to begin discussions on its use of Clearview AI, and will work with the Privacy Commissioner to develop guidelines and policies on the future use of automated facial recognition technologies.

Facial Recognition

Issue: Toronto Star article entitled “RCMP admits to using Clearview AI, say controversial facial recognition tool has solved child exploitation cases”

Proposed Response:

- Privacy is paramount and a reasonable expectation for Canadians, though this must be balanced with the ability of law enforcement to conduct investigations and protect the safety and security of Canadians.
- The RCMP is constantly monitoring new and evolving technologies in order to keep pace with the evolving methods of criminals, particularly in the area of online child sexual exploitation.
- The RCMP will be engaging with the Privacy Commissioner to work in partnership on the development of guidelines to ensure that our policies continue to conform to legislation and regulations.

Responsive:

- We are unable to comment further on operational matters relating to the RCMP.

Facial Recognition

Background

Recently, a number of media outlets have reported that some law enforcement agencies in Canada are either using or exploring facial recognition software to identify victims of crime or individuals involved in criminal activity. One application garnering significant media attention, is an American software application known as Clearview AI that makes use of publically available images and any associated meta data for its comparison process. Privacy concerns regarding the Clearview AI stem primarily from the open source comparisons being made via media collected via open source social media, and the manner in which these comparisons are being made, handled and retained.

The Toronto Star published an article on February 27, 2020 entitled "RCMP admits to using Clearview AI, say controversial facial recognition tool has solved child exploitation cases". The RCMP's National Child Exploitation Crime Centre (NCECC) has two paid licenses for the Clearview AI application and been using the technology since October 24, 2019. NCECC use has been limited to victim identification for investigations of online child sexual exploitation. Since acquiring these licenses, 15 child exploitation investigations have used the Clearview AI application, resulting in the successful identification and rescue of two children.

Additionally, there has been limited use of the Clearview AI application on a trial basis within a few units of the RCMP to determine its utility to support criminal investigations.

Civil liberty and privacy advocates have renewed their concerns around the legality of law enforcement's use of biometric technologies, including facial recognition, particularly around how the information is collected, used, disclosed, and retained. This has led the OPC to initiate an investigation into whether Clearview AI is in compliance with Canadian privacy legislation and develop guidance for organizations, including law enforcement on the use of biometric technology including facial recognition.

While traditional facial recognition tools, for example, mugshots, have been used by police in criminal investigations for decades, technological advances in areas such as biometrics, machine learning and artificial intelligence (AI) have led to the development of more advanced and sophisticated automated facial recognition technology, which can dramatically reduce the amount of time spent manually reviewing potential matches.

Automated facial recognition tools are capable of identifying or verifying an individual by comparing and analysing patterns, shapes and proportions of their facial features and contours. This is a relatively new technology and some law enforcement agencies are using it to support criminal investigations. For example, the INTERPOL Face Recognition System (IFRS) contains facial images received from more than 160 countries which makes it a unique global criminal database.¹

The RCMP has been engaged by the Office of the Privacy Commissioner to begin discussion on its use of the Clearview AI application, and will continue to work with the Privacy Commissioner to develop guidelines and policies on the future use of automated facial recognition technologies.

Contacts:

Prepared by: Kees Bradley, Manager, Cybercrime and Information Sharing Policy, 613-843-5877

Approved by: Stephen White, Deputy Commissioner, Specialized Policing Services, 613-843-4631

¹ <https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition>

Reconnaissance faciale

Sujet : Article du *Toronto Star* intitulé « RCMP admits to using Clearview AI, say controversial facial recognition tool has solved child exploitation cases »

Réponse suggérée :

- La protection de la vie privée est primordiale et constitue une attente raisonnable de la part de la population canadienne; toutefois, elle doit être mise en balance avec la capacité des organismes d'application de la loi de mener des enquêtes et d'assurer la sécurité des Canadiens et des Canadiennes.
- La GRC surveille constamment les technologies nouvelles et en constante évolution; cependant, le gouvernement ne révèle pas d'information sur les techniques et les outils précis que la police utilise.
- La GRC travaille en partenariat avec le commissaire à la protection de la vie privée pour mettre à l'essai deux programmes sous licence pour identifier les auteurs et les victimes de crimes

Responsive :

- Nous ne sommes pas en mesure de formuler d'autres commentaires sur des questions opérationnelles liées à la GRC.

Reconnaissance faciale

Contexte

Récemment, un certain nombre de médias ont rapporté que des organismes d'application de la loi au Canada utilisent ou examinent des logiciels de reconnaissance faciale pour identifier les victimes de crimes ou les personnes impliquées dans des activités criminelles. Les médias se sont beaucoup intéressés à Clearview AI, une application logicielle américaine qui utilise des images disponibles publiquement et toutes les métadonnées qui s'y rattachent pour son processus de comparaison. Les préoccupations en matière de protection de la vie privée concernant Clearview AI découlent principalement des comparaisons de sources ouvertes effectuées par l'intermédiaire de médias sociaux à source ouverte, et de la manière dont ces comparaisons sont faites, traitées et conservées.

Le *Toronto Star* a publié le 27 février 2020 un article intitulé « RCMP admits to using Clearview AI, say controversial facial recognition tool has solved child exploitation cases ». Le Centre national des crimes d'exploitation d'enfants (CNCEE) de la GRC dispose de deux licences payantes pour l'application Clearview AI et utilise la technologie depuis le 24 octobre 2019. L'utilisation qu'en fait le CNCEE est limitée à l'identification des victimes pour les enquêtes sur l'exploitation sexuelle des enfants en ligne. Depuis l'acquisition de ces licences, l'application Clearview AI a été utilisée dans 15 enquêtes sur l'exploitation des enfants, ce qui a permis d'identifier et de sauver deux enfants.

De plus, l'application Clearview AI a été utilisée de manière limitée, à titre d'essai, dans quelques groupes de la GRC afin de déterminer son utilité à l'appui d'enquêtes criminelles.

Les défenseurs des libertés civiles et de la vie privée ont réitéré leurs préoccupations concernant la légalité de l'utilisation de la technologie biométrique par les organismes d'application de la loi, y compris la reconnaissance faciale, plus particulièrement en ce qui concerne la manière dont les renseignements sont recueillis, utilisés, communiqués et conservés. Par conséquent, le Commissariat à la protection de la vie privée a ouvert une enquête pour déterminer si Clearview AI est conforme à la loi canadienne sur la protection de la vie privée et pour élaborer des lignes directrices à l'intention des organisations, y compris les services de police, sur l'utilisation de la technologie biométrique, notamment la reconnaissance faciale.

La police utilise des outils traditionnels de reconnaissance faciale, par exemple, les photos signalétiques, dans les enquêtes criminelles depuis des décennies, mais les progrès technologiques dans des domaines tels que la biométrie, l'apprentissage automatique et l'intelligence artificielle (IA) ont mené au développement d'une technologie de reconnaissance faciale automatisée plus avancée et plus sophistiquée, laquelle peut réduire considérablement le temps passé à examiner manuellement les correspondances possibles.

Les outils de reconnaissance faciale automatisés aident à identifier une personne ou à vérifier son identité en comparant et en analysant les caractéristiques, les formes et les proportions des traits et des contours de son visage. Il s'agit d'une technologie relativement nouvelle et certains organismes d'application de la loi l'utilisent à l'appui d'enquêtes criminelles. Par exemple, le système de reconnaissance faciale d'INTERPOL contient des images faciales provenant de plus de 160 pays, ce qui en fait une base de données criminelles mondiale unique².

La GRC s'est vu demander par le Commissariat à la protection de la vie privée d'entamer une discussion sur son utilisation de l'application Clearview AI et elle continuera de collaborer avec le commissaire à la protection de la vie privée à l'élaboration de lignes directrices et de politiques sur l'utilisation future de technologies de reconnaissance faciale automatisées.

Personnes-ressources :

Préparée par : Kees Bradley, gestionnaire, Cybercriminalité et Politique sur l'échange d'information, 613-843-5877
Approuvée par : Stephen White, sous-commissaire, Services de police spécialisés, 613-843-4631

² <https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition>